

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2001-22642

(P2001-22642A)

(43)公開日 平成13年1月26日(2001.1.26)

(51)Int.Cl.⁷

G 0 6 F 12/14

識別記号

3 1 0

3 2 0

F I

G 0 6 F 12/14

テ-マ-ト*(参考)

3 1 0 F 5 B 0 1 7

3 2 0 C

審査請求 未請求 請求項の数9 OL (全 8 頁)

(21)出願番号

特願平11-194904

(22)出願日

平成11年7月8日(1999.7.8)

(71)出願人 000006013

三菱電機株式会社

東京都千代田区丸の内二丁目2番3号

(72)発明者 中平 小百合

東京都千代田区丸の内二丁目2番3号 三

菱電機株式会社内

(74)代理人 100066474

弁理士 田澤 博昭 (外1名)

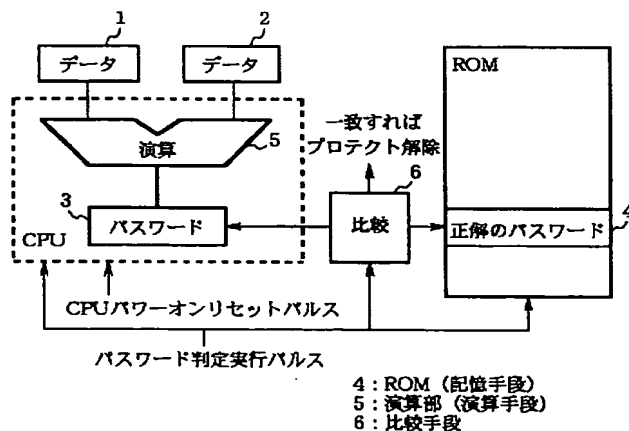
Fターム(参考) 5B017 AA02 BA05 CA12

(54)【発明の名称】 メモリの機密保持回路

(57)【要約】

【課題】 書き換え可能なROMに記憶されているデータの容易かつ不正な書き換えを防止する。

【解決手段】 外部から入力された複数のデータに対し所定のアルゴリズムを用いて演算を行い、入力パスワードとしての演算結果を出力する演算部5と、正解のパスワードを記憶した書き換え可能なROM4と、前記演算部5で演算した演算結果である前記入力パスワードと、前記ROM4に記憶した前記正解のパスワードとを比較し、一致した場合に限り、前記ROM4に格納されたデータに対し書き換えを禁止しているプロテクト機能を解除可能にする比較手段6とを備える。



【特許請求の範囲】

【請求項1】 外部から入力された複数のデータに対し所定のアルゴリズムを用いて演算を行い、入力パスワードとしての演算結果を出力する演算手段と、

正解のパスワードを記憶した記憶手段と、
前記演算手段で演算した演算結果である前記入力パスワードと、前記記憶手段に記憶した前記正解のパスワードとを比較し、一致した場合に限り、書き換え可能なROMに格納されたデータに対し書き換えを禁止しているプロテクト機能を解除可能にする比較手段と、
を備えたメモリの機密保持回路。

【請求項2】 演算手段は、外部から入力された複数のデータに対しハードウェアにより実現された所定のアルゴリズムを用いて演算を行うことを特徴とする請求項1記載のメモリの機密保持回路。

【請求項3】 演算手段は、外部から入力されたデータと、書き換え可能なROMに予め格納されたデータに対し所定のアルゴリズムを用いて演算を行い、入力パスワードとしての演算結果を出力することを特徴とする請求項1または請求項2記載のメモリの機密保持回路。

【請求項4】 正解のパスワードを記憶した記憶手段は、書き換え可能なROMであることを特徴とする請求項1から請求項3のうちのいずれか1項記載のメモリの機密保持回路。

【請求項5】 複数のデータは、電源投入後の所定期間内においてのみ、外部から入力ポートを介して入力することを特徴とする請求項4記載のメモリの機密保持回路。

【請求項6】 正解のパスワードは、電源投入の回数に対応してROMに予め複数記憶されており、
比較手段は、
前記ROMに記憶した複数の正解のパスワードから、今回の電源投入が何回目であるかに応じて選択した正解のパスワードと、演算手段で演算した演算結果である入力パスワードとを比較し、一致した場合に限り、前記ROMに格納されたデータに対し書き換えを禁止しているプロテクト機能を解除可能にすることを特徴とする請求項5記載のメモリの機密保持回路。

【請求項7】 電源投入の回数に対応した複数の正解のパスワードを記憶しておき、前記複数の正解のパスワードから、今回の電源投入が何回目であるかに応じて、その回数に応じて選択した正解のパスワードと、電源投入後の所定期間内においてのみ外部から入力した入力パスワードとを比較し、一致した場合に限り、書き換え可能なROMに格納されたデータに対し書き換えを禁止しているプロテクト機能を解除可能にするメモリの機密保持回路。

【請求項8】 正解のパスワードは、電源投入の回数に対応して書き換え可能なROMに予め複数記憶されており、前記ROMに記憶した複数の正解のパスワードから、今回の電源投入が何回目であるかに応じて、その回数に応じて選択した正解のパスワードと、電源投入後の所定期間内においてのみ外部から入力した入力パスワードとを比較し、一致した場合に限り、前記ROMに格納されたデータに対し書き換えを禁止しているプロテクト機能を解除可能にすることを特徴とする請求項7記載のメモリの機密保持回路。

【請求項9】 正解のパスワードを所定のレジスタへ記憶する際に、前記正解のパスワードを電源オフ時にバックアップされているRAMに保存し登録し、次の電源投入時には、クリアされた前記レジスタへ前記RAMに保存した正解のパスワードを書き込み、該正解のパスワードと外部から入力した入力パスワードとを比較し、一致した場合に限り、書き換え可能なROMに格納されたデータに対し書き換えを禁止しているプロテクト機能を解除可能にするメモリの機密保持回路。

【発明の詳細な説明】**【0001】**

【発明の属する技術分野】この発明は、メモリの機密保持回路に関し、特に電氣的にデータの書き込みと消去が可能なROMであるフラッシュメモリなどに用いて好適な、書き込まれているデータの容易かつ不正な書き換えを防止できるメモリの機密保持回路に関するものである。

【0002】

【従来の技術】従来のメモリの機密保持回路としては、例えば特開平2-300834号公報の半導体装置、特開昭63-316399号公報のコピー禁止機能を有する読出専用メモリなどに開示されたものがある。

【0003】従来、フラッシュメモリに書き込まれているデータのプロテクト、すなわち不正な状況下でのデータの書き換えを防止するプロテクト機能の作動および解除は、プロテクト制御レジスタへの所定データの書き込み、またはある外部端子へ与える信号レベルにより制御する構成が一般的に多く採用されている。

【0004】前記特開平2-300834号公報に開示された半導体装置では、半導体装置のメモリへ与えられたアドレスと、該アドレスにより前記メモリから読み出されたデータとを演算処理し、この演算処理結果を前記メモリの内容の読出結果として外部出力することで、解読しなければメモリの内容を知ることができず、前記メモリの内容が容易に不特定多数のものに理解されないようにし、前記メモリの内容の容易かつ不正な書き換えを困難にしたものである。

【0005】また、特開昭63-316399号公報に開示されたコピー禁止機能を有する読出専用メモリは、電源立ち上がり後の一定時間だけ電氣的にメモリの一部

ヘデータの書き込みが可能になるようにして、さらに照合データを書き込み、その照合データと予め前記メモリに書き込まれている暗号データとを比較し、一致すれば、前記メモリの全エリアを読み出し可能にすることで、前記メモリの内容についてのコピー、前記メモリの内容の容易かつ不正な書き換えを困難にしたものである。

【0006】

【発明が解決しようとする課題】従来のメモリの機密保持回路は以上のように構成されているので、メモリに書き込まれている内容が簡単に書き換えられてしまうものであってはならず、技術の進歩に従ってより高度なプロテクト機能の実現を図る必要性が求められているという課題があった。

【0007】この発明は上記のような課題を解決するためになされたものであり、書き換え可能なROMに記憶されているデータの容易かつ不正な書き換えを防止するプロテクト機能をより強化できるメモリの機密保持回路を得ることを目的とする。

【0008】

【課題を解決するための手段】この発明に係るメモリの機密保持回路は、外部から入力された複数のデータに対し所定のアルゴリズムを用いて演算を行い、入力パスワードとしての演算結果を出力する演算手段と、正解のパスワードを記憶した記憶手段と、前記演算手段で演算した演算結果である前記入力パスワードと、前記記憶手段に記憶した前記正解のパスワードとを比較し、一致した場合に限り、書き換え可能なROMに格納されたデータに対し書き換えを禁止しているプロテクト機能を解除可能にする比較手段とを備えるようにしたものである。

【0009】この発明に係るメモリの機密保持回路は、外部から入力された複数のデータに対しハードウェアにより実現された所定のアルゴリズムを用いて演算を行う構成を備えるようにしたものである。

【0010】この発明に係るメモリの機密保持回路は、外部から入力されたデータと、書き換え可能なROMに予め格納されたデータに対し所定のアルゴリズムを用いて演算を行い、入力パスワードとしての演算結果を出力する構成を備えるようにしたものである。

【0011】この発明に係るメモリの機密保持回路は、正解のパスワードを記憶した記憶手段として書き換え可能なROMを用いる構成を備えるようにしたものである。

【0012】この発明に係るメモリの機密保持回路は、電源投入後の所定期間内においてのみ、外部から入力ポートを介して複数のデータを入力するようにしたものである。

【0013】この発明に係るメモリの機密保持回路は、正解のパスワードが電源投入の回数に対応してROMに予め複数記憶されており、前記ROMに記憶した複数の

正解のパスワードから、今回の電源投入が何回目であるかに応じて選択した正解のパスワードと、電源投入後の所定期間内に外部から入力した複数のデータをもとに所定のアルゴリズムで演算した演算結果である入力パスワードとを比較し、一致した場合に限り、前記ROMに格納されたデータに対し書き換えを禁止しているプロテクト機能を解除するようにしたものである。

【0014】この発明に係るメモリの機密保持回路は、電源投入の回数に対応した複数の正解のパスワードを記憶しておき、前記複数の正解のパスワードから、今回の電源投入が何回目であるかに応じて、その回数に応じて選択した正解のパスワードと、電源投入後の所定期間内においてのみ外部から入力した入力パスワードとを比較し、一致した場合に限り、書き換え可能なROMに格納されたデータに対し書き換えを禁止しているプロテクト機能を解除可能にする構成を備えるようにしたものである。

【0015】この発明に係るメモリの機密保持回路は、正解のパスワードが電源投入の回数に対応して書き換え可能なROMに予め複数記憶されており、前記ROMに記憶した複数の正解のパスワードから、今回の電源投入が何回目であるかに応じて、その回数に応じて選択した正解のパスワードと、電源投入後の所定期間内においてのみ外部から入力した入力パスワードとを比較し、一致した場合に限り、前記ROMに格納されたデータに対し書き換えを禁止しているプロテクト機能を解除可能にする構成を備えるようにしたものである。

【0016】この発明に係るメモリの機密保持回路は、正解のパスワードを所定のレジスタへ記憶する際に、前記正解のパスワードを電源オフ時にバックアップされているRAMに保存し登録し、次の電源投入時には、クリアされた前記レジスタへ前記RAMに保存した正解のパスワードを書き込み、該正解のパスワードと外部から入力した入力パスワードとを比較し、一致した場合に限り、書き換え可能なROMに格納されたデータに対し書き換えを禁止しているプロテクト機能を解除可能にする構成を備えるようにしたものである。

【0017】

【発明の実施の形態】以下、この発明の実施の一形態について説明する。

実施の形態1. 図1はこの実施の形態1のメモリの機密保持回路の構成を示すブロック図である。図において、1および2は外部から入力ポートを介して入力されたデータ、3は演算部5に入力されたデータ1とデータ2の演算結果であり、入力されたパスワードとして用いられる。4は正解のパスワードであり、例えばフラッシュメモリのような書き換え可能なメモリ（記憶手段）（以下、ROMという）の所定のアドレスエリアに記憶されている。5は演算部（演算手段）、6は前記データ1とデータ2の演算結果と前記正解のパスワードとを比較

し、一致するとROM4に対し書き換えを禁止しているプロテクト機能を解除可能にする比較手段である。

【0018】次に動作について説明する。このメモリの機密保持回路では、フラッシュメモリのプロテクト解除のパスワードを、外部から直接入力されたデータによって決めるのではなく、演算部5で得られた演算結果として得られるパスワードによってのみにより受け付けるものである。

【0019】すなわち、比較データとなる正解のパスワード4を予めROMに格納しておき、外部から入力ポートを介して2つのデータ1、2を入力し、演算部5で演算処理された演算結果3をパスワードとして、この演算処理結果3と正解のパスワード4とを比較し、一致することでプロテクト機能を解除する。

【0020】なお、この演算処理結果がオーバーフローしたり、除算で商が零になった場合には、それ以降、ROMの書き換えを禁止するなどの条件を付与することで、プロテクト機能はさらに強化されることになる。

【0021】以上のように、この実施の形態1によれば、エンドユーザにおいてROMの書き換えが容易に行われてしまうことがなくなり、また、ROMの不正な書き換えも有効に防止できるメモリの機密保持回路が得られる効果がある。

【0022】実施の形態2。図2はこの実施の形態2のメモリの機密保持回路の機能を説明するための説明図である。図において、(a)は電源投入時におけるCPUの電源電圧の立ち上がり状態を示す波形図であり、電源が投入されると最初所定の待機数で立ち上がり、電源電圧VDDに安定する。また同図(b)は、電源投入時に図示していないパワーオンリセット回路により生成されるパワーオンリセットパルスを示す波形図であり、電源投入後、所定の期間T、Highレベルのパルスとして出力される。同図(c)は、電源投入時にCPUをリセットするためのCPUパワーオンリセットパルスを示す波形図である。このCPUパワーオンリセットパルスは、同図(b)に示すパワーオンリセットパルスが電源電圧VDDに安定してから所定の期間t ($t < T$) 出力される。同図(d)は、パスワードの判定が行われる期間を規定するパスワード判定実行パルスを示す波形図である。このパスワード判定実行パルスは、電源投入後、前記CPUパワーオンリセットパルスの出力が終了するまでの前記期間tが経過した後、前記パワーオンリセットパルスの出力が終了するまでのT-tの期間、出力されるパルスである。

【0023】次に、この実施の形態2のメモリの機密保持回路の動作について説明する。この実施の形態2のメモリの機密保持回路では、図2(d)に示すパスワード判定実行パルスが出力されている期間、前記実施の形態1で説明した2つのデータ1、2を外部から入力ポートを介して受け付ける。このため前記2つのデータ1、2

は前記期間に入力される。そして、この2つのデータ1、2を演算部5で演算処理し、その演算結果3をパスワードとして、この演算結果3と正解のパスワード4とを比較して、この比較結果をもとに一致すればプロテクト機能を解除する。

【0024】従って、この実施の形態2によれば、前記2つのデータ1、2を外部から入力ポートを介して入力する期間が前記パスワード判定実行パルスが出力されている期間内に限定され、さらに前記2つのデータの演算結果をパスワードとして正解のパスワードと比較するため、エンドユーザによる容易なROMの書き換え、ROMの不正な書き換えをより有効に防止できるメモリの機密保持回路が得られる効果がある。

【0025】実施の形態3。図3はこの実施の形態3のメモリの機密保持回路を説明するためのROMに複数個書き込まれた正解のパスワードを示す説明図である。図3では、正解のパスワードが5個、書き込まれている。このパスワードは電源投入の回数に応じて正解のパスワードが電源投入1回目の正解のパスワード1から例えば5回目の正解のパスワード5まで順次切り替えられる。すなわち、1回目の電源投入時にはパスワード1が正解のパスワードであり、2回目の電源投入時にはパスワード2が正解のパスワードになる。

【0026】次に動作について説明する。この実施の形態3のメモリの機密保持回路では、1回目の電源投入である場合、その電源投入後の図2(d)に示すパスワード判定実行パルスが出力されている期間、入力ポートを介してパスワードを入力し、このパスワードを図3に示す正解のパスワード1と比較し、この比較結果をもとに一致すればプロテクト機能を解除する。

【0027】同様に2回目の電源投入である場合、その電源投入後の図2(d)に示すパスワード判定実行パルスが出力されている期間、外部から入力ポートを介してパスワードを入力し、このパスワードを図3に示す正解のパスワード2と比較して、この比較結果をもとに一致すればプロテクト機能を解除する。

【0028】従って、この実施の形態3によれば、前記パスワードを外部から入力ポートを介して入力する期間が前記パスワード判定実行パルスが出力されている期間内に限定されるとともに、電源投入の回数に応じて正解のパスワードが切り替えられるため、エンドユーザによる容易なROMの書き換え、ROMの不正な書き換えをより有効に防止できるメモリの機密保持回路が得られる効果がある。

【0029】実施の形態4。図3はこの実施の形態4のメモリの機密保持回路を説明するためのROMに複数個書き込まれた正解のパスワードを示す説明図である。図3では、正解のパスワードが5個、書き込まれている。このパスワードは電源投入の回数に応じて正解のパスワードが電源投入1回目の正解のパスワード1から例えば

5回目の正解のパスワード5まで順次切り替えられる。すなわち、1回目の電源投入時にはパスワード1が正解のパスワードであり、2回目の電源投入時にはパスワード2が正解のパスワードになる。また、この正解のパスワードを用いたプロテクト解除は、前記実施の形態2で説明した構成により実現する。

【0030】ここで、この実施の形態4のメモリの機密保持回路の動作について説明すると、1回目の電源投入である場合、その電源投入後の図2(d)に示すパスワード判定実行パルスが出力されている期間、前記実施の形態1で説明した2つのデータ1、2を外部から入力ポートを介して入力し、この2つのデータ1、2を演算部5で演算処理し、その演算結果3をパスワードとして、この演算結果3と図3に示す正解のパスワード1とを比較して、この比較結果をもとに一致すればプロテクト機能を解除する。

【0031】同様に2回目の電源投入である場合、その電源投入後の図2(d)に示すパスワード判定実行パルスが出力されている期間、前記実施の形態1で説明した2つのデータ1、2を外部から入力ポートを介して入力し、この2つのデータ1、2を演算部5で演算処理し、その演算結果3をパスワードとして、この演算結果3と図3に示す正解のパスワード2とを比較して、この比較結果をもとに一致すればプロテクト機能を解除する。

【0032】従って、この実施の形態4によれば、前記2つのデータ1、2を外部から入力ポートを介して入力する期間が前記パスワード判定実行パルスが出力されている期間内に限定されるとともに、電源投入の回数に応じて正解のパスワードが切り替えられるため、エンドユーザによる容易なROMの書き換え、ROMの不正な書き換えをより有効に防止できるメモリの機密保持回路が得られる効果がある。

【0033】実施の形態5。この実施の形態5のメモリの機密保持回路は、最初、所定の手順でレジスタに書き込まれた正解のパスワードを電源オフ時バックアップされているRAMの所定領域にハードウェア的に転送し保存、登録しておき、次の電源立ち上げ時からは前記RAMから所定のレジスタへ前記正解のパスワードを書き込むようにする。そして、前記レジスタに書き込まれた正解のパスワードと、電源投入時に入力ポートから入力したパスワードとを比較して、一致すればプロテクト解除が行われる。

【0034】前記レジスタに書き込まれた正解のパスワードは、通常、電源投入時に前記レジスタがクリアされることで消失してしまうため、電源投入時にクリアされない前記RAMの所定領域へ正解のパスワードを転送することで正解のパスワードの消失を回避できる。

【0035】図4はこの実施の形態5のメモリの機密保持回路の機能を説明するための説明図である。図において、(a)は電源投入時におけるCPUの電源電圧の立

ち上がり、および立ち下がりの状態を示す波形図であり、電源が投入されると最初所定の時定数で立ち上がり、電源電圧VDDに安定する。また、電源オフの場合にも所定の時定数でグラウンド電位へ下降する。また同図(b)は、電源投入時に図示していないパワーオンリセット回路により生成されるパワーオンリセットパルスを示す波形図であり、電源投入後、所定の期間T、Highレベルのパルスとして出力される。同図(c)は、電源投入時にCPUをリセットするためのCPUパワーオンリセットパルスを示す波形図である。このCPUパワーオンリセットパルスは、同図(b)に示すパワーオンリセットパルスが電源電圧VDDに安定してから所定の期間t($t < T$)出力される。

【0036】また、図4の(d)は、電源投入時、前記RAMから前記レジスタへ正解のパスワードを転送する正解パスワード転送パルスである。同図(e)は、パスワードの判定が行われる期間を規定するパスワード判定実行パルスを示す波形図である。このパスワード判定実行パルスは、電源投入後、前記CPUパワーオンリセットパルスの出力が終了するまでの前記期間tが経過した後、前記パワーオンリセットパルスの出力が終了するまでのT-tの期間、出力されるパルスである。そして、このパスワード判定実行パルスが出力されている期間内に、入力ポートから入力したパスワードと前記レジスタへ転送された正解のパスワードとが比較される。また、同図(f)は、電源オフ時に前記レジスタから前記RAMへ正解のパスワードを転送するための正解パスワード転送パルスである。

【0037】以上のように、この実施の形態5によれば、最初、レジスタに正解のパスワードを書き込む所定の手順をエンドユーザが容易に知り得ないものにしておくことで、最初に前記レジスタへ正解のパスワードを書き込んだ者のみが正解のパスワードを知り得ることになり、前記最初に正解のパスワードを書き込んだ者以外の者は正解のパスワードを知ることができないため、エンドユーザによる容易なROMの書き換え、ROMの不正な書き換えをより有効に防止できるメモリの機密保持回路が得られる効果がある。

【0038】なお、電源立ち上げ時に前記RAMから所定のレジスタへ書き込まれる前記正解のパスワードが、前記実施の形態3、前記実施の形態4で説明したように電源投入が何回目かに応じて変化するような構成にすることで、エンドユーザによる容易なROMの書き換え、ROMの不正な書き換えをさらに有効に防止できるメモリの機密保持回路が得られる効果がある。

【0039】また、以上の説明では、電源オフ時に正解のパスワードが電源投入時クリアされないRAM領域へ転送される構成であったが、最初、所定の手順で前記レジスタへ正解のパスワードを外部から書き込み、このとき同時に前記レジスタに書き込んだパスワードを電源投

入時クリアされないRAM領域へハードウェア的に転送しておき、次の電源投入時以降からは、図4(a), (b), (c), (d)に示すように電源立ち上げ時に前記RAMから前記所定のレジスタへ正解のパスワードが書き込まれる構成であってもよい。

【0040】このように構成した場合にも、レジスタに正解のパスワードを書き込む前記所定の手順をエンドユーザが容易に知り得ないものにしておくことで、最初に前記レジスタへ正解のパスワードを書き込んだ者のみが正解のパスワードを知り得ることになり、前記最初に正解のパスワードを書き込んだ者以外の者は正解のパスワードを知ることができないため、エンドユーザによる容易なROMの書き換え、ROMの不正な書き換えをより有効に防止できるメモリの機密保持回路が得られる効果がある。

【0041】実施の形態6. 以上説明した各実施の形態では、パスワードの読解をCPUが行うものであったが、CPUではなくROM制御回路自身が行う構成であってもよい。CPUがパスワードの読解を行う構成の場合、書き換え可能なROMの内容を吸い出して逆アセンブルすることで読解の手法が明らかになってしまうため、ROM制御回路においてハードウェア的にプロテクトする。このような構成にすることでハードウェア的により安全なプロテクト機能を実現できる効果がある。

【0042】実施の形態7. 以上説明した実施の形態1などにおいては、データ1およびデータ2は、入力ポートを介して外部から入力される構成であったが、一方のデータは入力ポートから入力する構成であり、他方のデータは予めROMの所定のアドレス領域に記憶させておく構成であってもよい。また、正解のパスワードと比較するパスワードの元となるデータの数も、複数個であれば2個に限ることはない。

【0043】

【発明の効果】以上のように、この発明によれば、外部から入力された複数のデータに対し所定のアルゴリズムを用いて演算を行い、その演算結果として入力パスワードを得て、該入力パスワードと記憶手段に記憶した正解のパスワードとを比較し、一致した場合に限り、書き換え可能なROMに格納されたデータに対し書き換えを禁止しているプロテクト機能を解除可能にするように構成したので、前記正解のパスワードを知ることができても、前記複数のデータと前記アルゴリズムを知らない限り、前記正解のパスワードに合致する入力パスワードを生成することが困難であり、プロテクト機能を解除できず、書き換え可能なROMに記憶されているデータの容易かつ不正な書き換えを有効に防止できる効果がある。

【0044】この発明によれば、外部から入力された複数のデータに対しハードウェアにより実現された所定のアルゴリズムを用いて演算を行うように構成したので、ソフトウェアにより実現されたアルゴリズムと異なり、

アルゴリズムの内容を外部から読み出ししたりすることが困難であり、書き換え可能なROMに記憶されているデータの容易かつ不正な書き換えを有効に防止できる効果がある。

【0045】この発明によれば、外部から入力されたデータと、書き換え可能なROMに予め格納されたデータに対し所定のアルゴリズムを用いて演算を行い、その演算結果を入力パスワードとするように構成したので、正解のパスワードと合致する入力パスワードを前記アルゴリズムにより生成するための複数のデータおよびその入力について複雑化することが可能となり、書き換え可能なROMに記憶されているデータの容易かつ不正な書き換えを有効に防止できる効果がある。

【0046】この発明によれば、正解のパスワードを記憶した記憶手段として書き換え可能なROMを用いるように構成したので、正解のパスワードを容易に知ることが困難であり、書き換え可能なROMに記憶されているデータの容易かつ不正な書き換えを有効に防止できる効果がある。

【0047】この発明によれば、電源投入後の所定期間内においてのみ、外部から入力ポートを介して複数のデータを入力するように構成したので、正解のパスワードと合致する入力パスワードを前記アルゴリズムにより生成するための複数のデータの入力について複雑化することが可能となり、書き換え可能なROMに記憶されているデータの容易かつ不正な書き換えを有効に防止できる効果がある。

【0048】この発明によれば、正解のパスワードが電源投入の回数に対応してROMに予め複数記憶されており、前記ROMに記憶した複数の正解のパスワードから、今回の電源投入が何回目であるかに応じて選択した正解のパスワードと、電源投入後の所定期間内に外部から入力した複数のデータをもとに所定のアルゴリズムで演算した演算結果である入力パスワードとを比較し、一致した場合に限り、前記ROMに格納されたデータに対し書き換えを禁止しているプロテクト機能を解除するように構成したので、正解のパスワードと合致する入力パスワードを得るための条件が複雑化され、書き換え可能なROMに記憶されているデータの容易かつ不正な書き換えをより有効に防止できる効果がある。

【0049】この発明によれば、電源投入の回数に対応した複数の正解のパスワードを記憶しておき、前記複数の正解のパスワードから、今回の電源投入が何回目であるかに応じて選択した正解のパスワードと、電源投入後の所定期間内においてのみ外部から入力した入力パスワードとを比較し、一致した場合に限り、書き換え可能なROMに格納されたデータに対し書き換えを禁止しているプロテクト機能を解除可能にするように構成したので、正解のパスワードが電源投入のたびに变化し、入力パスワードの入力について複雑化でき、書き換え可能な

ROMに記憶されているデータの容易かつ不正な書き換えを有効に防止できる効果がある。

【0050】この発明によれば、正解のパスワードが電源投入の回数に対応して書き換え可能なROMに予め複数記憶されており、前記ROMに記憶した複数の正解のパスワードから、今回の電源投入が何回目であるかに応じて選択した正解のパスワードと、電源投入後の所定期間内においてのみ外部から入力した入力パスワードとを比較し、一致した場合に限り、前記ROMに格納されたデータに対し書き換えを禁止しているプロテクト機能を解除可能にするように構成したので、正解のパスワードを外部から容易に読み出すことができず、また正解のパスワードが電源投入のたびに变化するため、入力パスワードおよびその入力について複雑化でき、書き換え可能なROMに記憶されているデータの容易かつ不正な書き換えを有効に防止できる効果がある。

【0051】この発明によれば、正解のパスワードを所定のレジスタへ記憶する際に、前記正解のパスワードを電源オフ時にバックアップされているRAMに保存し登録し、次回の電源投入時には、クリアされた前記レジスタへ前記RAMに保存した正解のパスワードを書き込み、該正解のパスワードと外部から入力した入力パス

ワードとを比較し、一致した場合に限り、書き換え可能なROMに格納されたデータに対し書き換えを禁止しているプロテクト機能を解除可能にするように構成したので、最初に前記レジスタへ正解のパスワードを書き込んだ者のみが正解のパスワードを知り得ることになり、前記最初に正解のパスワードを書き込んだ者以外の者は正解のパスワードを知ることができず、容易なROMの書き換え、ROMの不正な書き換えをより有効に防止できる効果がある。

【図面の簡単な説明】

【図1】 この発明の実施の形態1のメモリの機密保持回路の構成を示すブロック図である。

【図2】 この発明の実施の形態2のメモリの機密保持回路の機能を説明するための説明図である。

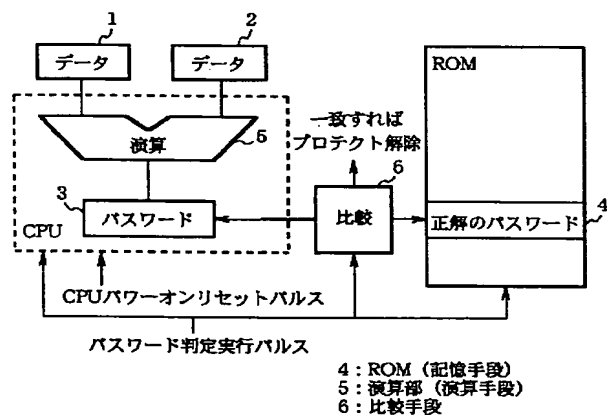
【図3】 この発明の実施の形態3および実施の形態4のメモリの機密保持回路を説明するためのROMに複数個書き込まれた正解のパスワードを示す説明図である。

【図4】 この発明の実施の形態5のメモリの機密保持回路の機能を説明するための説明図である。

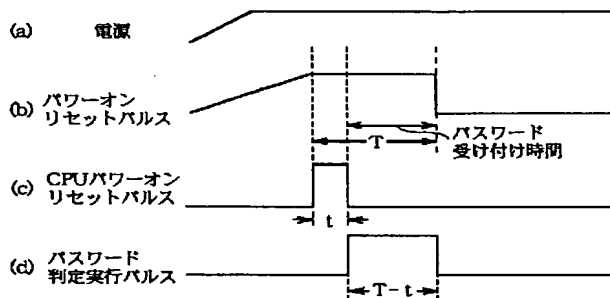
【符号の説明】

4 ROM（記憶手段）、5 演算部（演算手段）、6 比較手段。

【図1】



【図2】



【図3】

ROM	
正解のパスワード1 1回目
正解のパスワード2 2回目
正解のパスワード3 3回目
正解のパスワード4 4回目
正解のパスワード5 5回目

【図4】

